PESCO umsetzen – Handlungsfeld Cyber

Ralph D. Thiele

August 2017

Zusammenfassung

Im Juni 2017 hat der Europäische Rat beschlossen, dass die Mitgliedstaaten bis Ende September 2017 eine Liste mit Vorschlägen für eine konkrete Ausgestaltung der PESCO (Permanent Structured Cooperation) vorlegen. EuroDefense Deutschland schlägt vor, die PESCO durch gemeinsame Ausbildung im Handlungsfeld „Cyber" zu stärken. Die European Defence Agency (EDA) bietet sich hierfür als eine zweckmäßige Ausbildungsinstanz an. Partner aus Industrie und Forschung sollten ausdrücklich eingebunden werden. Mit Blick auf die Nutzung des Innovationspotenzials im Mittelstand schlägt EuroDefense Deutschland vor, periodisch – beispielsweise jährlich – eine Art „*Innovationsbörse*" einzurichten, bei der dieser Industriesektor die Möglichkeit erhält, konkret seine Ideen vorzustellen.

Das ISPSW

Das Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung (ISPSW) ist ein privates, überparteiliches Forschungs- und Beratungsinstitut.

In einem immer komplexer werdenden internationalen Umfeld globalisierter Wirtschaftsprozesse, weltumspannender politischer, ökologischer und soziokultureller Veränderungen, die zugleich große Chancen, aber auch Risiken beinhalten, sind unternehmerische wie politische Entscheidungsträger heute mehr denn je auf den Rat hochqualifizierter Experten angewiesen.

Das ISPSW bietet verschiedene Dienstleistungen – einschließlich strategischer Analysen, Sicherheitsberatung, Executive Coaching und interkulturelles Führungstraining – an.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analyse

1. Rasante Entwicklungen

Mit dem Vertrag von Lissabon (2009) haben die Mitgliedstaaten der Europäischen Union einen schrittweisen Entwicklungsprozess von nationalen hin zu europäisch integrierten, umfassenden Sicherheits- und Verteidigungskräften ermöglicht. Hierfür bietet die PESCO einen angemessenen Rahmen. Am 23.6. 2017 hat der Europäische Rat beschlossen, dass die Mitgliedstaaten bis Ende September 2017 eine Liste mit Vorschlägen für eine konkrete Ausgestaltung der PESCO vorlegen. Diese sollen mit einem konkreten Zeitplan für ihre Umsetzung versehen werden.

Im Kontext des gewandelten Sicherheitsumfelds und neuartiger, hybrider Bedrohungen spielt die Nutzung des Informationsraumes eine Schlüsselrolle. Die digitale Revolution hat die rasante Entwicklung einer Vielzahl qualitativ neuer Informations- und Kommunikationssysteme mit sich gebracht. Militärische Waffentechnik und militärische Planungs- und Führungsprozesse verändern sich von Grund auf. Neben den klassischen Räumen Land, Luft, See und Weltraum wird auch der Cyber-Space zum Operationsraum. Dabei liegt der entscheidende Bereich für Cybersicherheit – einschließlich militärischer Cybersicherheit – weitgehend außerhalb des Militärischen. Eine ressortübergreifende, ganzheitliche konzeptionelle Betrachtung ist dringend geboten.

Bereits am 18.5.2017 hatte sich der Rat der Europäischen Union schriftlich auf das angestrebte *„Ziel der PESCO"* festgelegt: *„die europäische Sicherheit und Verteidigung ... stärken"*. Hierfür sollen *„konkrete gemeinsame Projekte und Initiativen ermittelt werden."* (9178/17) EuroDefense Deutschland unterbreitet hierzu im Handlungsfeld „Cyber" einen Vorschlag sowie daran angelehnt einen Vorschlag zur Nutzung der Innovationskompetenz von KMUs.

2. Handlungsfelder

Für die EU Mitgliedstaaten selbst lautet die Herausforderung, die in Art 42, Abs. 6 [EUV] angesprochene PESCO von der Theorie in praktisches Handeln zu überführen. Aus Sicht EuroDefense Deutschland verdienen folgende Handlungsfelder besonderes Augenmerk:

- Kräfte/Fähigkeiten der ersten Stunde

  Das Konzept der EU-Battlegroups ist überarbeitungsbedürftig. Bislang fehlen zivile und militärische Kräfte/Fähigkeiten für Stabilisierungs-/Auslandseinsätze oder im Falle der „Beistandsklausel" (Artikel 42 [EUV] und Artikel 222 [AEUV]), die in einer unvorhergesehenen Notlage sofort eingreifen können. Darüber hinaus fehlt auch ein gemeinsames Verständnis für deren Nutzung.

- Krisenbewältigung („Auslandseinsätze") und Führungsfähigkeit der EU

  Eine Kernkompetenz der EU ist die abgestimmte Nutzung ziviler und militärischer Mittel zur Krisenbewältigung. Für den zivilen Bereich gibt es schon seit längerem einen Führungsstab, nicht jedoch für den militärischen. Dieser ist im Verbund mit dem schon vorhandenen zivilen Kommando optimal als ein zivil-militärisches EU-Kommando für die strategisch-operative Planung, Vorbereitung und Führung aufzustellen.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

- Äußere und Innere Sicherheit

  Durch grenzüberschreitenden internationalen Terrorismus, Organisierte Kriminalität und bestimmte Formen hybrider Kriegführung verschwimmen die Grenzen zwischen Innerer und Äußerer Sicherheit. Für Strategische Frühwarnung, ein ständig aktualisiertes Lagebild und verzugsarme Abstimmung der Einsätze nationaler bzw. internationaler Kräfte (Nachrichtendienste, Militär, Grenzschutz, Polizei) sowie europäischer Agenturen (Frontex, EuroPol, EDA, EU-Satellitenzentrum) bedarf es einer ständigen, resilienten, organisatorischen Lösung, insbesondere auch für den Grenz- und Küstenschutz.

- Gemeinsame Ausbildung

  Die Ausbildung der Sicherheits- und Verteidigungskräfte sollte im Kontext der PESCO vereinheitlicht und effizienter gemacht werden. Neben der dadurch erzielbaren Kostenersparnis ist die Einheitlichkeit im operativen und taktischen Denken der einbezogenen zivilen und militärischen Kräfte und deren Zusammenwirken von besonderem Wert. Voraussetzung hierfür ist, dass sich die PESCO-Staaten über gemeinsame Anforderungen für Einsatz, Ausbildung und ggf. Ausrüstung einig werden.

- Cyber

  Die Sicherheit der Netzwerke herzustellen und zu garantieren, ist eine der größten Herausforderungen im Rahmen der zunehmenden Vernetzung von zivilen und militärischen Sicherheitskräften und Entscheidungsträgern und damit auch der PESCO. Der Schutz kritischer Infrastrukturen beispielsweise wirkt systemkritisch hinsichtlich der Anforderungen Äußerer und Innerer Sicherheit in den einzelnen Mitgliedstaaten wie auch von EU und NATO insgesamt.

3. Gemeinsame Ausbildung im Handlungsfeld "Cyber"

EuroDefense Deutschland schlägt vor, die PESCO durch gemeinsame Ausbildung im Handlungsfeld „Cyber" zu stärken.

Zur Begründung: Wer selbstkritisch die zahlreichen Unzulänglichkeiten im Umgang mit der Domäne Cyber analysiert, muss feststellen, dass einer der gewichtigsten Mängel bei den Entscheidungsträgern nationaler Sicherheit und Verteidigungspolitik liegt. Diese verstehen die Chancen und Risiken der Informationstechnologie sowie Herausforderungen bei der Begrenzung von zugehörigen Risiken nur unzulänglich. Auf der anderen Seite verstehen die fachlichen technischen Experten zu wenig vom konzeptionellen und politischen Rahmen. Dementsprechend wäre die EU gut beraten, zivile und militärische Führungskräfte aller ihrer Institutionen bis hinunter zu mittleren Führungsebenen umfassend in Cybersicherheit zu bilden, auszubilden und zu trainieren. Sie kann hier bereits auf bestehende Grundlagen wie das von der NATO empfohlene Referenzcurriculum „Cybersicherheit" zurückgreifen und auch nationale Initiativen wie das entstehende Cyber Cluster mit Forschung und Wirtschaft rund um die Universität der Bundeswehr in München einbinden.

Folgende Themenkomplexe bieten sich an:

- Der Cyberraum und Grundlagen der Cybersicherheit
- Risikovektoren
- Zusammenhang defensiver und offensiver Cyber-Fähigkeiten
- Nationale und internationale Cybersicherheit Organisationen, Politiken und Standards
- Cybersicherheitsmanagement im nationalen und internationalen Kontext.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

- Technische Attributionsmöglichkeiten und politische Implikationen

Hands-on Training und Umgang mit Technologie sollten dabei ein Gespür für praktische Herausforderungen vermitteln. Scenario Training sowie Kollaboration und Kommunikation im Team stärken Sensibilität und Können für spätere Führungsaufgaben. Auch hohe Führungsebenen sind einzubeziehen. Gerade deren Lernerfolg bewirkt systemische Verbesserungen. Simulation gestützte Übungen im ressortübergreifenden, multinationalen Kontext bereiten für die erfolgreiche Bewältigung konkreter Führungsaufgaben umfassend vor.

Die European Defence Agency (EDA) hat seit ihrer Gründung den Auftrag, *„den Rat und die Mitgliedstaaten in ihren Bemühungen um die Verbesserung der Verteidigungsfähigkeiten der EU im Bereich der Krisenbewältigung zu unterstützen und die GSVP, wie sie sich gegenwärtig darstellt und in Zukunft entwickelt, dauerhaft zu unterstützen*". Sie bietet sich damit auch im Handlungsfeld *„Cyber*" als eine zweckmäßige Ausbildungsinstanz an. Hier wird allerdings von Anfang an darauf zu achten sein, dass ein ganzheitlicher Ansatz alle –auch die mehrheitlich nicht militärischen – Stakeholder einbindet. Dies ist nicht zuletzt deshalb bedeutsam, dass künftig zivile und militärische Bedarfsträger und Bedarfsdecker konsequenter Cybersicherheitsvorgaben in die Spezifikationen von Beschaffungsvorhaben hineinschreiben.

4. Mittelstand

Die Ausbildung im Handlungsfeld *„Cyber*" sollte die Partner aus Industrie und Forschung ausdrücklich einbinden. Die großen Systemhäuser sind unentbehrlich mit ihren umfassenden Lieferketten und ihrer Fähigkeit, Regeln und Standards vorzugeben sowie mit größeren Vorabinvestitionen Entwicklungen voranzutreiben. Das entstehende Cyber Cluster um die Universität der Bundeswehr in München wurde bereits beispielhaft angeführt. Darüber hinaus kann insbesondere der Mittelstand wichtige Beiträge leisten, der großen Dynamik nationaler und internationaler Cyberherausforderungen erfolgreich zu begegnen.

In den Schlussfolgerungen des Rates der Europäischen Union vom 14. November 2016 bekräftigt dieser die Notwendigkeit, zur Umsetzung der Strategie der Europäischen Union im Bereich Sicherheit und Verteidigung eine *„stärker integrierte, tragfähigere, innovativere und wettbewerbsfähigere technologische und industrielle Basis der europäischen Verteidigung (EDTIB)*" zu schaffen. Er nimmt dabei Bezug auf entsprechende Schlussfolgerungen des Europäischen Rates vom Dezember 2013. Dabei soll die besonders ausgeprägte Innovationskompetenz kleiner und mittlerer Unternehmen (KMUs) viel mehr als bisher genutzt werden. Zwar hat es hier schon seit Jahren Bemühungen gegeben, dieses Potential beispielsweise durch die Institution eines Mittelstandsbeauftragen zu nutzen. Allerdings hat dies bislang nur im geringen Umfang zu einer nennenswerten Stärkung des Mittelstandes der sicherheitstechnischen Industrie in Deutschland geführt.

EuroDefense Deutschland schlägt vor, periodisch - beispielsweise jährlich - eine Art *„Innovationsbörse*" einzurichten, bei der dieser Industriesektor die Möglichkeit erhält, konkret seine Ideen vorzustellen. Bei besonderem industriepolitischen Interesse könnten die entsprechenden innovativen Ansätze der Industrie auch schwerpunktmäßig gebündelt werden. Eine Förderung mit öffentlichen Mitteln sollte in Erwägung gezogen werden. Die gemeinsame Ausbildung im Handlungsfeld Cyber bietet einen exzellenten Einstieg für eine Cyber bezogene Innovationsbörse.

***

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Anmerkungen: Der Beitrag gibt die persönliche Auffassung des Autors wieder.

Über den Autor dieses Beitrags

Oberst a.D. und Diplom-Kaufmann Ralph D. Thiele ist Vorsitzender der Politisch-Militärischen Gesellschaft e.V. (pmg), Berlin, CEO von StratByrd Consulting und seit März 2017 Präsident von EuroDefense (Deutschland). EuroDefense ist eine private und unabhängige Initiative engagierter und beruflich erfahrener Persönlichkeiten, die sich für die Gestaltung der europäischen Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) als Teil der Werte- und Interessensgemeinschaft des Nordatlantischen Bündnisses einsetzen.

In seiner militärischen Laufbahn war Herr Thiele in bedeutenden nationalen und internationalen, sicherheits- und militärpolitischen, planerischen und akademischen Verwendungen eingesetzt, darunter im Planungsstab des Verteidigungsministers, im Private Office des NATO-Oberbefehlshabers, als Chef des Stabes am NATO Defense College, als Kommandeur des Zentrums für Transformation und als Direktor Lehre an der Führungsakademie der Bundeswehr.

Eine Vielzahl von Publikationen, regelmäßige Vorträge in Europa, Amerika und Asien sowie eine intensive Forschungstätigkeit im Kontext deutscher, österreichischer und europäischer Sicherheitsforschung unterstreichen sein ausgeprägtes Kompetenzspektrum.

Ralph D. Thiele ist Mitglied im Beirat Deutscher Arbeitgeber Verband e.V., Wiesbaden und im Beirat der Zeitschrift für Außen- und Sicherheitspolitik, Köln.

Er gehört auch dem ISPSW Rednermanagement Team an. Weitere Informationen finden Sie auf der ISPSW Website unter http://www.ispsw.com/autoren-und-rednermanagement/

Ralph D. Thiele

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de